(12) UK Patent Application (19) GB (11) 2 214 677 (13) A

(43) Date of A publication 06.09.1989

(21) Application No 8801674.6

(22) Date of filing 26.01.1988

(51) INT CL⁴
H04N 7/167

(52) UK CL (Edition J)
G4H HNMC H1A H13D H14G H60
U1S S2206 S2209 S2212

(56) Documents cited
None

(58) Field of search
UK CL (Edition J) G4H HNMC, H4F FDE, H4R RCSC RCSS RCST
INT CL⁴ H04H, H04N

(71) Applicant
Philips Electronic & Associated Industries Limited

(Incorporated in the United Kingdom)

Arundel Great Court, 8 Arundel Street, London, WC2R 3DT, United Kingdom

(72) Inventor
Andrew Frank Mervyn Hone

(74) Agent and/or Address for Service
R J Boxall
Philips Electronics, Patents and Trade Marks Department, Centre Point, New Oxford Street, London, WC1A 1QJ, United Kingdom

(54) Decoding transmitted scrambled signals

(57) In a subscription television system a programme signal is transmitted scrambled to prevent its un authorised reception in an intelligible manner. A receiver for such a signal requires a group customer message or messages and in addition a unique customer message or messages for the descrambling of the scrambled programme signal. The group customer message is/are transmitted with the scrambled programme signal whilst the unique customer message or messages is/are conveyed to the receiver through the inclusion of an optical bar code or codes (47) which are read by a reading device (46) which is coupled to the receiver.

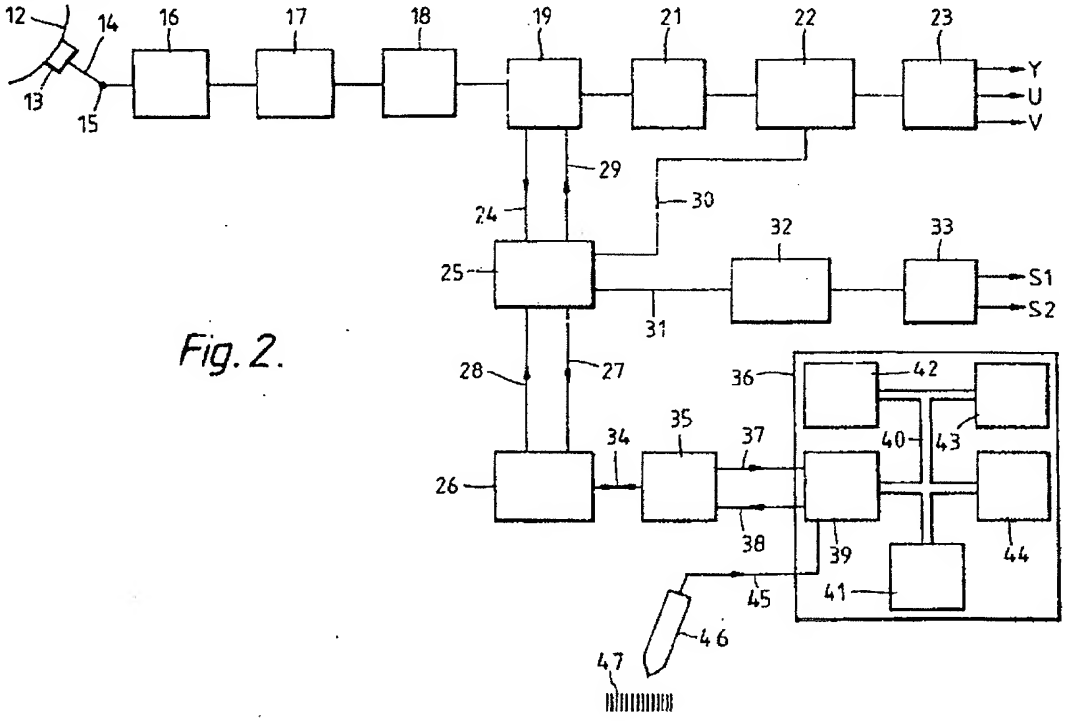


Fig. 2.

GB 2 214 677 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

2214677

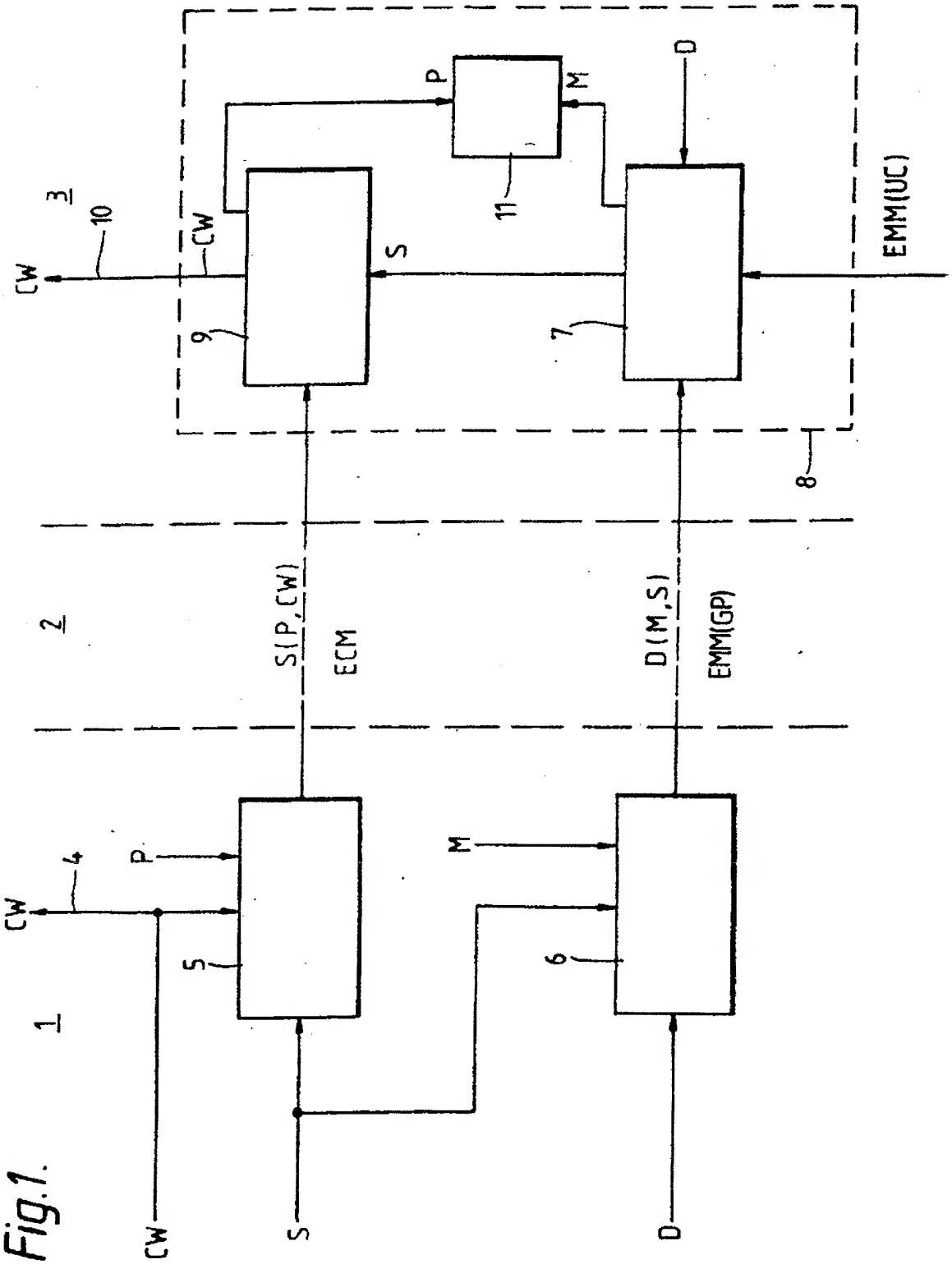


Fig.1.

2214677

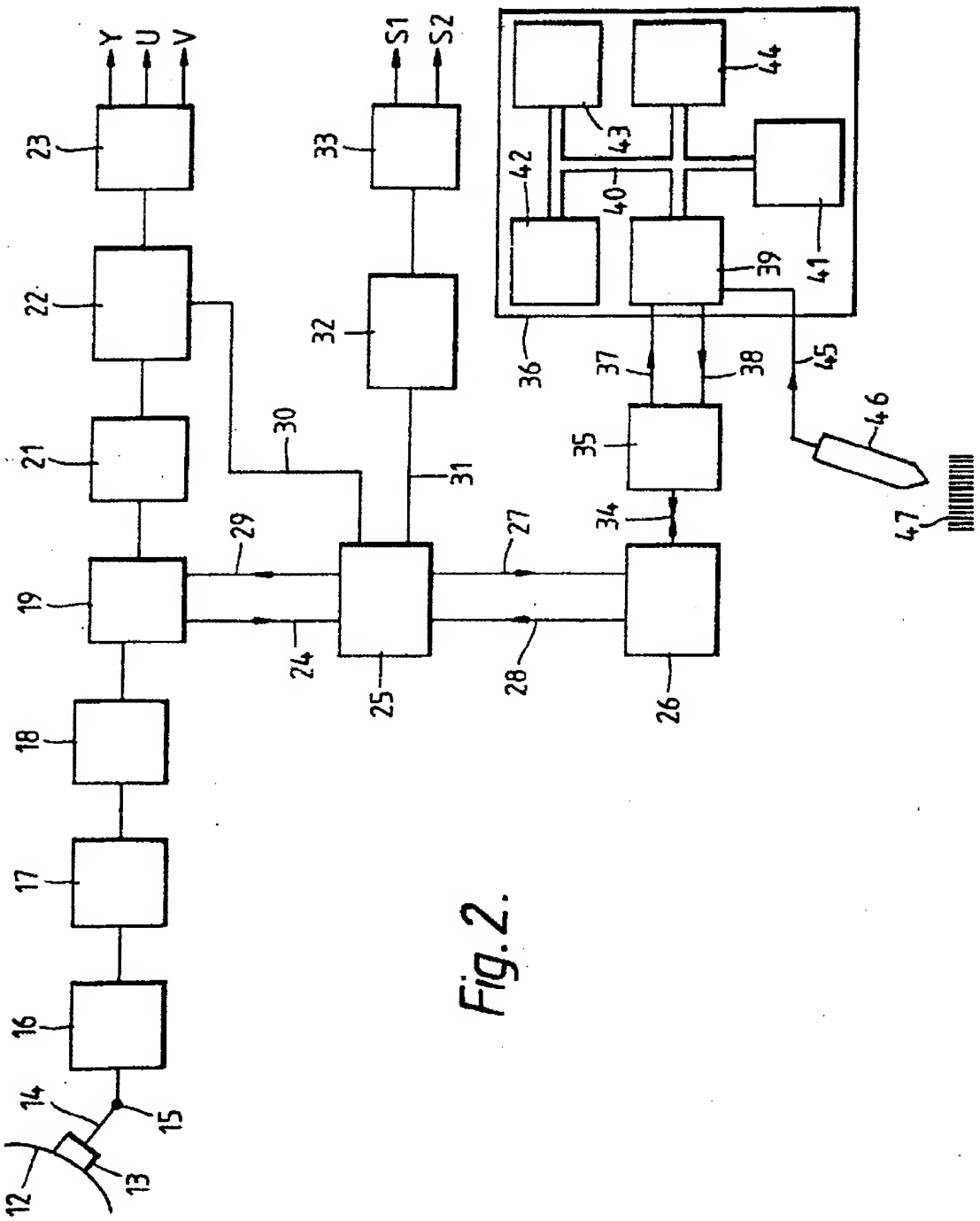
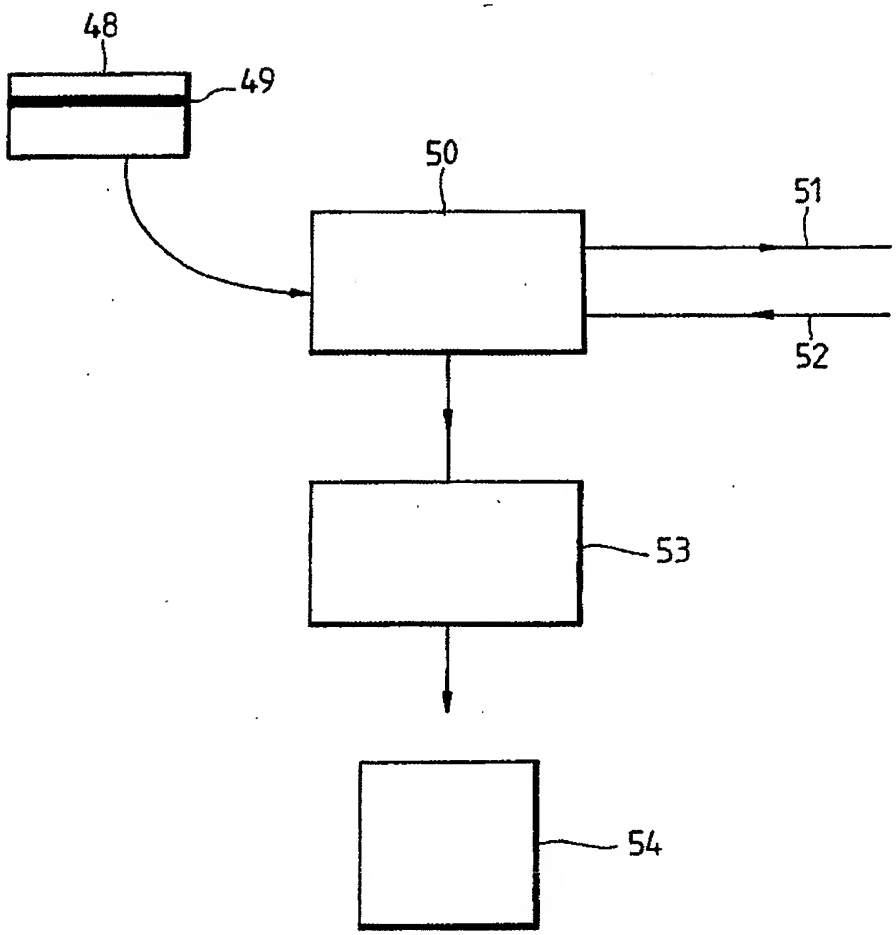


Fig. 2.

2214677

Fig.3.



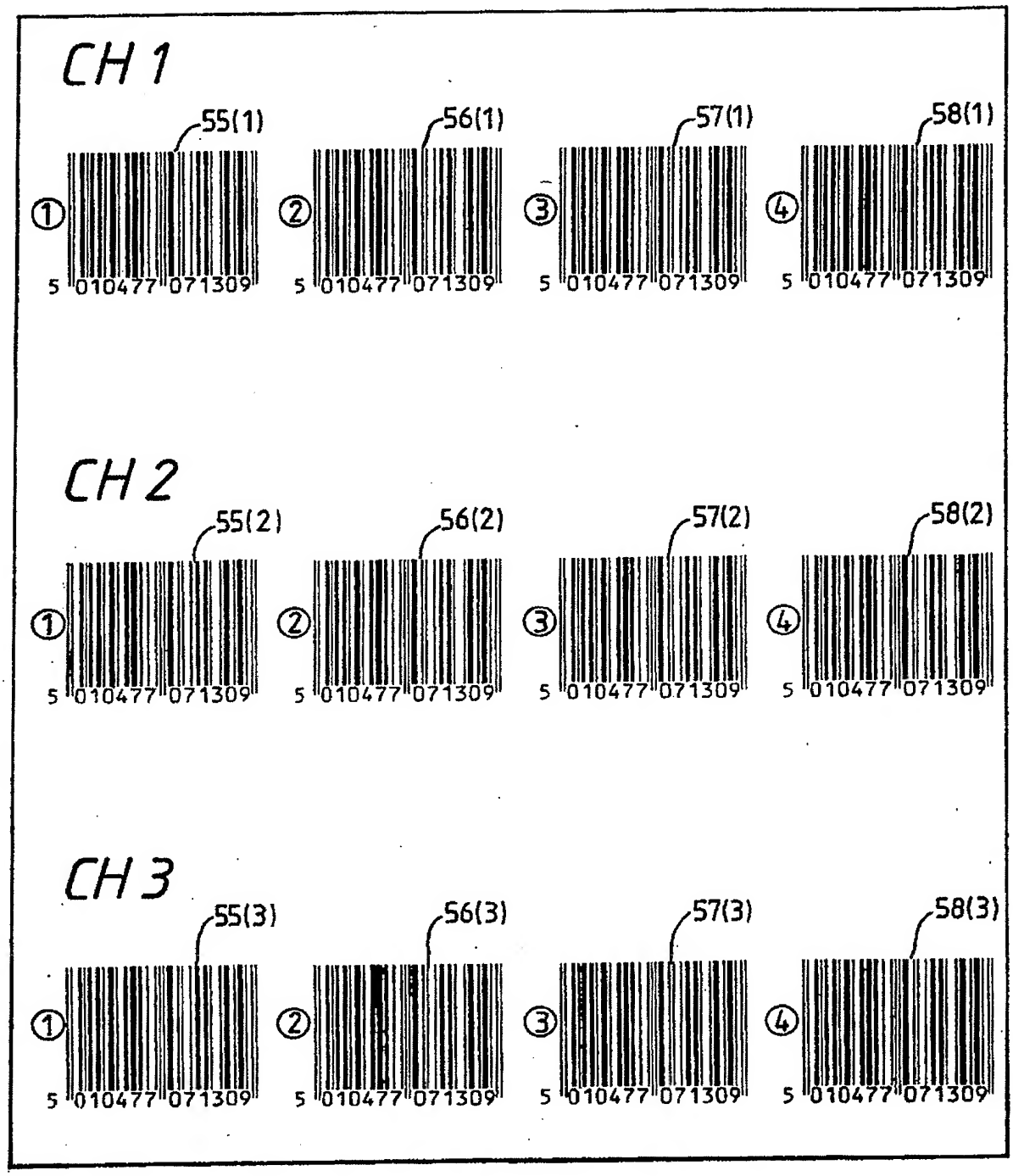


Fig.4.

DESCRIPTION:

"DECODING TRANSMITTED SCRAMBLED SIGNALS"

This invention relates to a method for enabling a receiver to decode a transmitted scrambled signal which relates to a programme such that said programme may be obtained in an intelligible manner. The invention also relates to apparatus for use with such a method.

A number of proposals have previously been made for authorising subscribers or subscribers' receivers to receive scrambled signals in an intelligible manner. Proposals for over-air addressing are contained in the European Broadcasting Union (EBU) document Tech. 325B-E "Specification of the systems of the MAC/packet family" of October 1986, which document is incorporated herein by way of reference. This document refers to a system, known as System B, which is a shared key over-air addressing system where the scrambling process i.e. the process that renders the picture and/or sound/data unintelligible, is derived from a truly random control word (CW1 or CW2). The control word and any programme data (P) are encrypted using a supplementary key (S) and the resulting cryptogram S(P,CW) is sent over-air in an Entitlement Checking Message (ECM). The Supplementary key(s) together with customer messages or authorisations (M) are further encrypted using a shared distribution key (D) and the resulting cryptogram D(M,S) is sent over-air an Entitlement Management Message (EMM). The shared distribution key is stored within the viewer's conditional access sub-system (CASS) which enables this sub-system to derive the Control Word or words, and to store any authorisations. The EMM has two data streams of which the Unique Customer messages are used to update the CASS in terms of shared distribution key, address, etc. and the Shared Customer messages contain the actual entitlements or authorisations.

With such a system it takes a finite time to authorise each subscriber to receiver a programme in an intelligible manner and with a limited number of subscribers and a limited number of channels in a television service the delay, if any, between a subscriber switching on his television receiving or switching to a particular channel appears, with current proposals, to be quite

acceptable especially where each channel of a serivce also carries the authorisations for the other channels. When we talk of a limited number of subscribers we are considering a satellite broadcast service being limited to a particular country which may have of the order to 10 million subscribers and with the service itself having, say, three channels. As originally conceived the transmissions for DBS (direct broadcast by satellite) services where subscribers would receive their signals direct from the satellite would have a footprint covering an area with a signal strength sufficient to produce a picture of an acceptable quality which would cover a single country or a group of small countries. However, with the considerable improvements that have been achieved in recent years in aerial head end amplifiers and down converters it has been found that the footprint for a given satellite would be considerably enlarged and such a footprint would be even greater in the case of cable operators using a more sophisticated aerial system and associated equipment than would be used by an individual subscriber. In addition to the proposed DBS transmissions there are current proposals for lower powered satellites that would have an even greater footprint. It is quite clear that future satellite television transmissions will be receivable over very large areas covering several countries and with a potential audience of say 100 million subscribers. With some large footprints subscriber's will be able to receive programmes from a number of satellites. All this increases the complexity of authorising subscribers and the time taken for subscribers to receive such authorisation following switch-on or a change of channel, which could make the access time to receive a programme in an intelligible manner totally unacceptable.

It is an object of the invention to provide a system and apparatus that can reduce such access time.

The invention provides a method for enabling a receiver to decode a transmitted scrambled signal which relates to a programme such that said programme may be obtained in an intelligible manner, wherein in order to decode said scrambled signal said receiver

requires, in addition to said scrambled signal, a group customer message or messages common to a group of receivers or customers and a unique customer message or messages unique to said receiver or a customer using said receiver, the group customer message or messages being conveyed to said receiver with the transmission containing said scrambled signal, characterised in that the unique customer message or messages is/are conveyed to said receiver through the medium of an optical bar code or codes.

Such a method has the advantage that it is no longer necessary to transmit the unique customer messages with the scrambled signal and as each receiver or customer requires at least one such message per service for a given period or even for a given programme there is a considerable saving in the amount of conditional access data that has to be transmitted. The access time to a programme can therefore be considerably reduced as the customer can insert these messages for various services at a time of his choosing.

The invention also provides a receiver for use with the above method, said receiver comprising means for receiving from a transmission a scrambled signal relating to a programme, means for receiving from said transmission a group customer message or messages relevant to said receiver or a customer using said receiver, means for receiving a unique customer message or messages unique to said receiver or said customer, means for descrambling said scrambled signal to provide said programme in an intelligible manner and descrambling control means for controlling the operation of said descrambling means under the control of said group customer message or messages and said unique customer message or messages, characterised in that said means for receiving said unique customer message or messges comprises optical reading means coupled to said receiver for reading the unique customer message or messages which are conveyed in the form of an optical bar code or codes and for transferring said unique customer message or messages into said receiver.

Such a receiver may further comprise a remote control unit for remotely controlling various functions of said receiver,

characterised in that said optical bar code reading means may be incorporated in said remote control unit.

The above and other features of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:-

Figure 1 is an idealised block diagram of a shared key addressing system for use with the invention,

Figure 2 is a block diagram of a receiver for use with the invention,

Figure 3 is a block diagram of apparatus for generating message carrying bar codes, and

Figure 4 is a diagrammatic representative of a sheet carrying a number of such bar codes.

The system of the present invention is based on the proposal for the System B access control system the practical implementation for which is described on page 221 etc. of EBU document Tech. 3258-E mentioned above. A detailed description to System B is not given herein and the reader is directed to this above document for an understanding of System B. In the following description the references used in relation to packets and blocks of data and their format are similar to those used in the document and detailed explanations will only be entered into where these differ from the disclosures.

With the System B proposal the Shared Customer Address (SCA) provides either the subscriber validation or authorisation in the subscription mode or loads tokens into the subscriber's controlled access sub-system in the pay-per-view mode. For a given programme it is not possible for different subscribers to gain entitlement to receive that programme in an intelligible manner by the two different modes nor for a subscriber not pre-authorised to receive that programme to gain access to it via the pay-per-view mode. With the present system both possibilities exist.

Figure 1 shows the shared-key over-air addressing system for System B which is based on Figure 3 appearing on page 236 of the above document. The figure is divided into three portions where

reference 1 denotes the parts contained on the transmission side, reference 2 a transmission path and 3 the parts contained on the receiver side which includes the controlled access sub-system. On the transmission side control words CW (which includes the control words CW1 and CW2) are applied via a connection 4 to a scrambling sequence generator (not shown) to control the scrambling of programme material, both sound and vision. The control word CW is also applied to a first encrypter 5 together with any programme data P and which is encrypted using a supplementary key S to produce at the output of encrypter 5 the cryptogram S(P,CW). The supplementary key S together with customer messages M are applied to a second encrypter 6 and which are encrypted using a distribution key D to produce at the output of encrypter 6 the cryptogram D(M,S). In the transmission path 2 the cryptogram S(P, CW) is conveyed in an entitlement checking message (ECM) whilst the cryptogram D(M,S) is conveyed in an entitlement management message (EMM). At the receiver side 3 a first decrypter 7 present in a security device 8 (receives the cryptogram D(M,S) from the EMM together with the distribution key D, the decrypter 7 producing the supplementary key S and any customer messages M at separate outputs. A second decrypter 9 receives the cryptogram S(P, CW) from the ECM together with the supplementary key S from decrypter 7 to produce at separate outputs the control word CW and any programme data P. The control word CW (which again includes the control words CW1 and CW2) is applied via a connection 10 to a descrambling sequence generator (not shown) to control the descrambling of the programme material. The customer message M and the programme data P from the respective outputs of decrypters 7 and 9 are applied to a store 11.

With the above system the EMM data stream conveys both group customer messages as well as unique customer messages. The group customer messages are relatively low in number as a group could comprise, say, all subscribers in a particular country and/or those subscribers wishing to obtain programmes relating to a particular class such as sport. The unique customer messages are relatively high in number as they address customers or subscribers individually

which means that with the small amount of data space available particularly in a D2-MAC/packet system after the sound channels have taken the space they require in the sound/data burst it could take an exceedingly long time to transmit all such unique customer messages. This could have the effect of preventing a subscriber from being able to view a programme for a considerable time following selection of a channel or switch on. In order to overcome this it is proposed that only the group customer messages should be conveyed by the EMM channel in the transmission path for which reason it is labelled EMM (GP) in Figure 1. As far as the unique customer messages are concerned it is further proposed that these should be entered into the receiver by the subscriber which obviates the delay in receipt of these from the transmitter 1. This is shown diagrammatically in Figure 1 by the further input to the first decryptor 7 from outside the receiver labelled EMM(UC).

A receiver using the present system is shown in Figure 2 for receiving signals from a D or D2-MAC packet transmission and where the reference 12 indicates a dish aerial suitable for receiving satellite television signals in the 12GHz band, the aerial having a down converter 13 attached to it which frequency converts the incoming television signal to a frequency within the 1 to 2GHz band depending of course on the frequency of the incoming signal. The down converted signal is applied over a co-axial cable 14 to a terminal 15 forming the input for the television receiver, this terminal 15 being connected to an r.f. amplifier and frequency changer stage 16 which amplifies and transforms the incoming signal to a suitable i.f. frequency of about 480MHz which is further amplified by an i.f. amplifier 17. The output of the amplifier 17 is applied to a frequency demodulator 18 as the components of the broadcast satellite television signal are frequency modulated, the demodulated output of the demodulator 18 being applied to an input of a MAC signal analogue processor unit 19 which separates the analogue vision components from the digital components of the MAC signal. The digital components provide synchronising information and various clock frequencies together with the sound/data and

control signals. The vision components from the analogue processor unit 19 are applied to an analog to digital converter 21 for conversion to digital form and thence applied to a vision decoder 22 where the luminance and chrominance vision components, subjected to line cut rotation scrambling at the transmission source, are descrambled and re-assembled for application to a digital to analog converter 23 to produce simultaneous analogue Y, U and V components for application to a matrix (not shown) prior to being prepared for display.

The data and clock signals from the digital portion of the MAC signal are applied from the analogue processor unit 19 over a connection 24 to a sync. control unit 25 where various data and synchronising information are processed under the control of a microprocessor 26. Such data are contained in certain areas of the multiplex such as the Service Information (SI) packets and data in line 625 and are applied to the microprocessor 26 over a connection 27. Control data for the sync. control unit 25 is applied from the microprocessor 26 over a connection 28. The sync. control unit 25 applies control data over a connection 29 to the analogue processor unit 19 to control the timing of the digital data to unit 25 and the analogue signals to converter 21 whilst a connection 30 applies control data to the vision decoder 22 to control the descrambling and assembly of the Y, U and V components of the vision signal. The latter control data will include the control word CW2 for application to a descrambling sequence generator controlling the descrambling of the vision components. Data and control signals, including the control word CW1 for application to a descrambling of the sound/data components, are applied over a connection 31 to a sound decoder 32 where the appropriate sound/data services are selected and descrambled, the sound/data signals having been subjected to scrambling at the transmission source by the addition of a pseudo random sequence using an exclusive OR-gate. The appropriate descrambled sound/data services are applied from the sound decoder 32 to a second digital to analog converter 33 to produce (say) two such services S1, S2 for reproduction.

The microprocessor 26 is additionally connected over a two way connection 34 to an interface 35 conveying the data needed for communication with a controlled access sub-system 36 which is connected by input (37) and output (38) connections. The sub-system 36 contains an interface 39 between the input and output connections 37, 38 and a bus 40. The bus 40 interconnects a central processor unit 41 with a read only-memory (ROM) 42 which provides the program for running the sub-system, a random access memory (RAM) 43 which stores data, and a non-volatile memory (NVM) 44 which provides long time storage for long term keys such as the Unique key and the Supplementary keys. It is the controlled access sub-system 36 in combination with the other parts of the receiver which controls which services may be received in an intelligible manner and the control software of the sub-system 36 is organised to that end. The controlled access sub-system 36 has a further input 45 which is connected into the interface 39. This input 45 is coupled to an optical reader 46 arranged to read an optical code such as a bar code 47. The bar code or codes 47 carry the EMM unique customer message for a particular channel or service for a given period, such as a month. The EMM group customer messages are introduced into the controller access sub-system 36 via the input 37 together with various ECM messages. As an alternative the input 45 may be connected through a suitable buffer to a different point within the receiver from which it can be directed into the controlled access sub-system 36.

The optical reader 46 may be built into the cabinet of the television receiver in which case the bar code will be carried by a suitable medium such as a tape so that it can be drawn over the reader. More conveniently the optical reader 46 may be in the form of a bar code reading pen connected to the receiver by a cable so that the pen can be readily drawn over a bar code or codes which may be carried on a paper sheet. As an alternative the bar code reading pen could be a stand-alone device which when drawn over the bar code or codes stores the coded information within itself and subsequently transmits these codes from the pen by means of an infra-red

transmitter and received by an infra-red receiver housed in the television receiver in the same manner as for a television remote control. In fact the reading pen could be incorporated in such a remote control unit and use the same infra-red transmitter housed in the remote control unit.

As the bar codes are effectively the authorisation for a programme to be received intelligibly for a channel for a given period and are unique to the receiver or the subscriber they will need to be provided by the organisation providing the programmes to be viewed. This could mean that a subscriber could end up receiving per period (say a month) a number of individual authorisations possibly on separate sheets each conveying the bar code or codes for a particular service. It would be more advantageous to the subscriber if he could obtain all the authorisations (bar codes) at a single place such as the shop where he purchased his television receiver or (say) a post office. In either case a laser printer could be provided to print the necessary bar codes which printer could be in direct contact with the various programme providers. As the unique customer messages are encrypted with the receiver's or the subscriber's unique key which in the former case can be buried within the subscriber's receiver (conveniently within an integrated circuit) and which is unique to that receiver it could be an advantage if the supply of the bar codes is at the shop where the receiver was purchased and where the subscriber's unique key could be retained. If the bar codes are supplied from some other place then it may be necessary for the subscriber to provide his/her unique key or that for the receiver and this may be conveniently achieved by a card which carries this magnetically, the card being normally kept by the subscriber. A simplified block diagram for such arrangement is shown in Figure 3.

In Figure 3 the reference 48 indicates a card, say of credit card size, which carries a magnetic strip 49 containing a magnetic imprint of the unique key. The card 48 is inserted into a coder unit 50 which is connected sequentially to a number of programme providers by means of the connection 51 over which a request is made

for that subscriber to receive programmes or a given tier or tiers of programmes. The requested authorisations are sent by the programmer provider(s) to the coder 50 over the connection 52 where these authorisations are encrypted by the unique key from the card 48. Alternatively, these authorisations may be encrypted by the unique key at the programme provider(s) if this unique key has already been sent over the connection 51. The encrypted authorisation prepared or received in coder 50 are passed to a printer 53 which prints the encrypted authorisation as bar codes on a sheet 54. These encrypted authorisations from the above unique customer messages. Obviously, the quality of the bar codes needs to be as high as possible and for this reason the printer 53 could suitably be a laser printer.

Figure 4 shows a form that the sheet 54 could take, where the sheet is divided into (say) three areas each relating to a separate programme provider each of which is distinguished by a channel number or other form of programme provider identification such as a name. In Figure 4 the three channels are identified by CH1, CH2 and CH3. Below each channel identification is a row of (say) four bar codes 55, 56, 57 and 58, the codes for a given channel being identified in parenthesis by the channel number. Each bar code includes 12 decimal digits such that the four bar codes in a row would provide 48 decimal digits. As each unique customer message could be accommodated in 39 decimal digits four such codes can provide more than enough such information. (Although in practice each bar code will be different for the sake of convenience all the bar codes shown in Figure 4 are identical). In using the sheet 54 the subscriber will cause the bar code reading pen 46 (Figure 2) to travel across the sheet from left to right in the numbered sequence shown circled.

From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the design, manufacture and use of systems and arrangements and component parts thereof and which may be used instead of or in addition to features

already described herein. Although claims have been formulated in this application to particular combinations of features, it should be understood that the scope of the disclosure of the present application also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present invention. The applicants hereby give notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present application or of any further application derived therefrom.

CLAIMS:

1. A method for enabling a receiver to decode a transmitted scrambled signal which relates to a programme such that said programme may be obtained in an intelligible manner, wherein in order to decode said scrambled signal said receiver requires, in addition to said scrambled signal, a group customer message or messages common to a group of receivers or customers and a unique customer message or messages unique to said receiver or a customer using said receiver, the group customer message or messages being conveyed to said receiver with the transmission containing said scrambled signal, characterised in that the unique customer message or messages is/are conveyed to said receiver through the medium of an optical bar code or codes.

2. A method for enabling a receiver to decode a transmitted scrambled signal substantially as herein described with reference to the accompanying drawings.

3. A receiver for use with a method as claimed in the preceding claims, said receiver comprising means for receiving from a transmission a scrambled signal relating to a programme, means for receiving from said transmission a group customer message or messages relevant to said receiver or a customer using said receiver, means for receiving a unique customer message or messages unique to said receiver or said customer, means for descrambling said scrambled signal to provide said programme in an intelligible manner and descrambling control means for controlling the operation of said descrambling means under the control of said group customer message or messages and said unique customer message or messages, characterised in that said means for receiving said unique customer message or messges comprises optical reading means coupled to said receiver for reading the unique customer message or messages which are conveyed in the form of an optical bar code or codes and for transferring said unique customer message or messages into said receiver.

4. A receiver as claimed in Claim 3 further comprising a remote control unit for remotely controlling various functions of

said receiver, characterised in that said optical bar code reading means is incorporated in said remote control unit.

5. A receiver substantially as herein described with reference to the accompanying drawings.

Published 1989 at The Patent Office, State House, 66/71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office, St Mary Cray, Orpington, Kent BR5 3RD. Printed by Multiplex techniques ltd, St Mary Cray, Kent, Con. 1/87